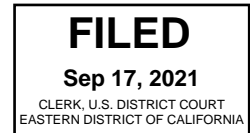


UNITED STATES DISTRICT COURT

for the
Eastern District of California



In the Matter of the Search of)
)
Hyundai SUV, with CA license plate 8UXX035)
and VIN KM8JU3AC1CU441924)
)

Case No. 2:21-sw-0733 AC

SEALED

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

SEE ATTACHMENT A-3, attached hereto and incorporated by reference.

located in the Eastern District of California, there is now concealed (*identify the person or describe the property to be seized*):

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. § 841(a)(1)	Distribution of a Controlled Substance
21 U.S.C. §§ 846, 841(a)(1)	Conspiracy to Distribute, and Possess with Intent to Dist., a Controlled Substance
18 U.S.C. § 2320(a)(4)	Trafficking in Counterfeit Goods and Services
18 U.S.C. § 1956(a)(1)(A)(i)	Money Laundering

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Christopher S. Fitzpatrick

Applicant's signature


Christopher S. Fitzpatrick, Special Agent, IRS-CI

Printed name and title

Sworn to me and signed via telephone.

Date: September 17, 2021

City and state: Sacramento, California


ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

**AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT
FOR JONATHAN PATRICK TURRENTINE; AND RELATED SEARCH WARRANTS**

I, Christopher Scott Fitzpatrick, being duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of the Department of Treasury, Internal Revenue Service – Criminal Investigation (“IRS-CI”) since September 2001. I am currently assigned to the IRS-CI Sacramento Office and I am charged with investigating drug trafficking and money laundering activities in the Eastern District of California, and elsewhere. I am a law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), and I am empowered by law to conduct investigations and make arrests for federal felony offenses. Additionally, I am a federal law enforcement officer within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure, that is, a federal law enforcement agent engaged in enforcing criminal laws and authorized to request a search warrant.

2. I was trained as a Federal Law Enforcement Training Center located in Glyncro, Georgia. During my training, I received special training in Money Laundering, including but not limited to, Title 18 United States Code Sections 1956 and 1957. I have also received special training in Specified Unlawful Activities, including but not limited to, Title 21 United States Code Sections 841(a)(1) and 846, Controlled Substance Violations and Conspiracy to Commit Controlled Substance Violations, respectively. I have also spoken to and worked with experienced federal, state, and municipal agents and narcotics officers regarding the methods and means employed by drug manufacturers and drug traffickers including the use of express carriers and the U.S. Postal system to distribute drugs.

3. During the course of my employment as a IRS-CI Special Agent, I have participated in numerous criminal investigations. I have participated in executing numerous Federal and State search warrants involving the aforementioned listed controlled substances, the seizure of narcotics-related records and other types of evidence that document the activities of criminal organizations in both the manufacturing and distribution of controlled substances, and

the money laundering of the criminally derived proceeds. To successfully conduct these investigations, I have utilized a variety of investigative techniques and resources, including physical and electronic surveillance, various types of infiltration, including undercover agents, informants, and cooperating sources. Through these investigations, my training and experience, and conversations with other agents and law enforcement personnel, I am familiar with the methods used by drug traffickers to smuggle and safeguard controlled substances, to distribute, manufacture, and transport controlled substances, and to collect and launder related proceeds.

4. I am part of the Northern California Illicit Digital Economy (“NCIDE”) task force composed of DEA, Homeland Security Investigations (“HSI”), the Federal Bureau of Investigation (“FBI”), the United States Postal Inspection Service (“USPIS”), and IRS-CI. As a function of this task force, investigators regularly purchase narcotics utilizing both digital and fiat currencies, from the persons operating and illegally selling narcotics on the “clear” portion of the internet, from the “dark” portion of the internet and from various social media platforms. Investigators conduct the undercover purchases of narcotics to assist in the effort to identify the suspects operating such illicit sites.

II. PURPOSE

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested complaint, arrest warrant, and search warrants and does not set forth all of my knowledge about this matter. Rather, I make this affidavit in support of applications for:

6. A criminal complaint and arrest warrant for Jonathan Patrick TURRENTINE, for violations of the following statutes (collectively, the “Subject Offenses”)

- i. 21 U.S.C. § 841(a)(1) (Distribution of a Controlled Substance);
- ii. 21 U.S.C. §§ 846, 841(a)(1) (Conspiracy to Distribute, and to Possess with Intent to Distribute a Controlled Substance);
- iii. 18 U.S.C. § 2320 (a)(4) (Trafficking in Counterfeit Goods and Services); and,
- iv. 18 U.S.C. § 1956 (a)(1)(A)(i) (Money Laundering):

- b. Warrants to search the following locations, for the seizure of items described in Attachment B:
- i. **9161 Tuolumne Drive, Sacramento, California (TARGET PROPERTY)**, further described in Attachment A-1;
 - ii. **a Toyota Avalon bearing California license plate number 8WQS507 and Vehicle Identification Number (“VIN”) 4T1BF12B7VU171416**, registered to Jonathan P. Turrentine (**TURRENTINE VEHICLE #1**), further described in Attachment A-2;
 - iii. **a Hyundai SUV bearing California license plate number 8UXX035 and VIN KM8JU3AC1CU441924**, registered to S.T. (hereafter referred to as **TURRENTINE VEHICLE #2**), further described in Attachment A-3;
 - iv. **The person of Jonathan Patrick TURRENTINE**, further described in Attachment A-4.

III. OVERVIEW

7. During this investigation, federal law enforcement officers have: (1) observed Jonathan Patrick TURRENTINE place parcels containing narcotics into the United States Postal Service (“USPS”) mail system; (2) conducted multiple undercover purchases of counterfeit Adderall and Xanax pills, ecstasy, LSD, marijuana, and compromised emails/passwords through a dark web marketplace vendor account; and (3) traced monies used in undercover narcotics purchases by law enforcement officers to financial accounts controlled by TURRENTINE. In doing so, TURRENTINE has committed the following federal violation.

- a) Manufacturing and distributing controlled substances.
 - i. Under 21 U.S.C. § 841(a)(1), “it shall be unlawful for any person knowingly or intentionally to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance.”
- b) Conspiring to manufacture and distribute controlled substances.
 - i. Under 21 U.S.C. § 846, “any person who attempts or conspires to commit any offense defined in this subchapter shall be subject to the

same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.”

- c) Trafficking in Counterfeit Goods or Services.
 - i. Under 18 U.S.C. § 2320, “whoever intentionally traffics in a drug and knowingly uses a counterfeit mark on or in connections with such drug or attempts or conspires to traffic in a counterfeit drug, shall be fined not more than \$2,000,000 or imprisoned not more than 10 years, or both.”
- d) Laundering monetary instruments.
 - i. Under 18 U.S.C. § 1956 (a)(1)(A)(i), “Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity, with the intent to promote the carrying on of specified unlawful activity, shall be sentenced to a fine of not more than \$500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both.”

IV. TECHNICAL BACKGROUND

8. Digital currency (also known as crypto-currency) is generally defined as an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e. currency created and regulated by a government.) Digital currency exists entirely on the Internet and is not stored in any physical form. Digital currency is not issued by any government, bank, or company and is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Digital currency is not illegal in the United States and may be used for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions, such as the sale of controlled substances.

9. Bitcoin¹ is a type of digital currency. Bitcoin payments are recorded in a public

¹ The value of Bitcoin fluctuates with supply and demand, much like any other currency, and it can often be volatile. Near the beginning of this investigation, on or around December 10, 2019, one Bitcoin was worth approximately \$7,230 USD. In mid-April 2021, Bitcoin was valued as high as nearly \$65,000 per Bitcoin, but, at the time of writing, one Bitcoin is worth approximately \$48,000 USD.

ledger that is maintained by peer-to-peer verification and is thus not maintained by a single administrator or entity. Individuals can acquire Bitcoins either by “mining” or by purchasing Bitcoins from other individuals. An individual can “mine” for Bitcoins by allowing his/her computing power to verify and record the Bitcoin payments into a public ledger. Individuals are rewarded for this by being given newly created Bitcoins.

10. An individual can send and receive Bitcoins through peer-to-peer digital transactions or by using a third-party broker. Such transactions can be done on any type of computer, including laptop computers and smart phones.

11. Bitcoins can be stored in digital “wallets.” A digital wallet essentially stores the access code that allows an individual to conduct Bitcoin transactions on the public ledger. To access Bitcoins on the public ledger, an individual must use a public address (or “public key”) and a private address (or “private key.”) The public address can be analogized to an account number while the private key is like the password to access that account.

12. Even though the public addresses of those engaging in Bitcoin transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public addresses are not recorded. If, however, a real individual or entity is linked to a public address, it would be possible to determine what transactions that individual or entity conducted. Bitcoin transactions are, therefore, described as “pseudonymous,” meaning they are partially anonymous.

13. Through the dark web or darknet, i.e. websites accessible only through encrypted means, individuals have established online marketplaces, such as the Silk Road, for narcotics and other illegal items. These markets often only accept payment through digital currencies, such as Bitcoin. Accordingly, a large amount of Bitcoin sales or purchases by an individual is often an indicator that the individual is involved in narcotics trafficking or the distribution of other illegal items. Individuals intending to purchase illegal items on Silk Road-like websites need to purchase or barter for Bitcoins. Further, individuals who have received Bitcoin as proceeds of illegal sales on Silk Road-like websites need to sell their Bitcoin to convert them to fiat (government-backed) currency. Such purchases and sales are often facilitated by peer-to-peer

Bitcoin exchangers who advertise their services on websites designed to facilitate such transactions.

14. Dark web sites, such as Silk Road, AlphaBay, Empire, and SamSara, operate on “The Onion Router” or “TOR” network. The TOR network (“TOR”) is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet Protocol (“IP”) addresses of the computers accessing the network, and, thereby, the locations and identities of the network’s users. TOR likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as “hidden services” on the TOR network. Such “hidden services” operating on TOR have complex web addresses, which are many times generated by a computer algorithm, ending in “.onion” and can only be accessed through specific web browser software designed to access the TOR network.

V. FACTS ESTABLISHING PROBABLE CAUSE

A. Background Investigation of CALIPLUGMIKE and Identification of Jonathan TURRENTINE as CALIPLUGMIKE

15. I am part of the Northern California Illicit Digital Economy (NCIDE) Task Force composed of personnel from DEA, Homeland Security Investigations (HSI), the Federal Bureau of Investigation (FBI), the United States Postal Inspection Service (USPIS), and the Internal Revenue Service Criminal Investigation Division (IRS-CI). As a function of this task force, investigators regularly purchase narcotics utilizing both digital and fiat currencies from persons illegally selling narcotics on the “clear” portion of the internet, as well as from those selling from the “dark” portion of the internet, and from various social media platforms. Investigators conduct the undercover purchases of narcotics to identify suspects operating such illicit sites.

16. In approximately December 2019, the Northern California Illicit Digital Economy (NCIDE) task force opened a joint investigation of a user identifying himself as “CALIPLUGMIKE,” a dark web vendor suspected of mailing controlled substances via the United States Postal Service (USPS). CALIPLUGMIKE offered products for sale via a vendor

site on a dark web marketplace for illicit sales known as Empire Market. CALIPLUGMIKE's site offered various quantities of LSD, cocaine, Xanax pills, Adderall pills, psilocybin mushrooms, ecstasy, and marijuana products in various forms, including edibles, vape pens/cartridges, and marijuana buds in gram, ounce, and pound quantities for sale.² He also offered for sale compromised emails and passwords. Over the course of this investigation, undercover agents purchased various items of contraband from CALIPLUGMIKE. Agents communicated with CALIPLUGMIKE via encrypted text messaging services such as Wickr and attempted execute direct deals with him. On Wickr, CALIPLUGMIKE utilizes the moniker "caliplugmike" to communicate with customers.

17. In approximately April 2018, an HSI agent identified Jonathan TURRENTINE as a possible dark web vendor of illegal merchandise. A search of TURRENTINE's criminal history revealed that TURRENTINE had a 2004 conviction for manufacturing/possessing a dangerous weapon, a 2004 arrest for possession of marijuana for sale, and, most recently, a 2017 arrest and conviction for illegal use/access of a computer data system. As reported by the Sacramento County District Attorney's Office, between October 22, 2016 and November 1, 2016, TURRENTINE and a co-conspirator, who were both employed by the State of California Department of Technology, utilized State of California computer systems to mine the digital currency Monero. In March 2018, TURRENTINE pleaded no contest to accessing illegally a computer network to obtain money, property, or data wrongfully, and was sentenced to 3 years of probation and 30 days in jail.

18. In November 2018, during a visual and informational exam of mail parcels arriving for delivery to the Sacramento, California area, USPIS Postal Inspectors observed a parcel with several anomalies that lead them to believe the parcel contained controlled substances and/or the proceeds of narcotics trafficking. The parcel was addressed to "John

² While Turrentine may have advertised pills for sale on his vendor site under the brand names of "Xanax" and "Adderall," it is likely that the pills were counterfeit pharmaceuticals that had not been produced by the company from which they purported to come but had instead been pressed by an illicit manufacturer using chemicals different from those the genuine pills would contain.

Turrentine” at 30 Arches Circle, Sacramento, California, with sender information of “Tan Dinh, 11843 Plumbrook Dr., Houston, Texas 77099.” USPS inspectors held the parcel for further investigation. On the same day, Tri-County Drug Enforcement Team (TRIDENT) Task Force Commander Brandon Olivera utilized his narcotics-detection canine to sniff the parcel at the Royal Oaks Post Office. The canine alerted to the odor of narcotics on the suspect parcel. Later that morning, USPS Inspector Bauwens and members of the TRIDENT task force arrived at 30 Arches Circle, Sacramento, California, the address on the suspect parcel. The owner of the home indicated that John TURRENTINE rented a room in the house. Agents then spoke with a male who identified himself as John TURRENTINE. TURRENTINE stated that he was not expecting any parcels and denied knowing anyone by the name of “Tan Dinh” or anyone else from Houston. TURRENTINE gave agents consent to open the parcel and inspect the contents. Upon opening the parcel, agents located several thousand white pills which appeared to be counterfeit Xanax tablets. TURRENTINE denied all knowledge of the pills and stated that he was not expecting any such delivery.

19. At the time of the delivery, investigators were aware that TURRENTINE was on informal searchable probation for unauthorized use/access of computer data/systems. Investigators conducted a search of the room TURRENTINE rented at the residence and discovered the following items:

- a) a green pill bottle containing 67 white tablets, identical to the pills that were located in the suspect parcel that had been addressed to TURRENTINE;.
- b) shipping/mailling items, including shipping envelopes and boxes, prepaid USPS shipping labels, a vacuum sealing machine, and unused vacuum sealed bags;
- c) marijuana vaping cartridges and suspected butane honey oil; and
- d) several computers and electronic devices.

20. During the probation search, investigators observed one computer with an active monitor on and observed communications which were consistent with that of an individual operating a darknet vendor site to distribute illegal narcotics. A cursory search of the computer

revealed that TURRENTINE controlled several dark web vendor accounts and utilized the monikers MUSHMIKE1776, CALICARTCONNECT, CALICARTS, BIGBOYCARTS, and CALIFORNIABUDZ. Additionally, investigators observed documents on the computer containing shipping labels with fictitious business names and addresses utilizing versions of the name “eBay Store.”

21. On December 9, 2019, a DEA Special Agent submitted the suspected counterfeit Xanax tablets (approximately 5,093 tablets; 1,126.3 grams (gross)), seized from the intercepted parcel destined for TURRENTINE, to the DEA Western Regional Laboratory (WRL). On January 13, 2020, WRL Senior Forensic Chemist Charmaine X. Qui reported that her analysis of one of the suspected Xanax tablets indicated that the tablet consisted of alprazolam and etizolam. The DEA Special Agent also submitted the 67 tablets agents had found in the green pill bottle in TURRENTINE’s bedroom. Senior Forensic Chemist Charmaine X. Qui’s analysis of one of the 67 tablets indicated that the tablet consisted of alprazolam.

22. On April 22, 2019, Sacramento Postal Inspectors were conducting routine profiling of suspected narcotics parcels and observed two packages which were mailed that same day at the Royal Oaks Post Office in Sacramento. The two parcels bore a fictitious return business name, “CPlus eBay Store,” similar to a return address found during the November 2018 search in the mailing materials on TURRENTINE’s computer. A US Postal Inspector reviewed the Self Service Kiosk (SSK) transactions associated with the purchase of the postage affixed to the two parcels, which indicated that the person who purchased the postage was TURRENTINE.

23. On December 2, 2019, a San Diego Postal Inspector notified Sacramento Postal Inspectors of a dark web narcotics vendor operating out of the San Diego area. The San Diego Inspector advised that the local dark web vendor was receiving suspected narcotics packages from the Sacramento area, bearing the fictitious return business name of “CC101 Parts.” The San Diego Inspector advised that the most recent parcel had been mailed from Sacramento on November 27, 2019. Again, the postage on the parcel was purchased from a Sacramento post office SSK. On December 2, 2019, Sacramento Postal Inspectors reviewed the images captured

on surveillance cameras from around the time of the SSK transaction and observed that the person who purchased the postage to ship the San Diego parcel was TURRENTINE.

24. In December 2019, Sacramento agents learned that the Orange County DEA office was investigating a dark web vendor utilizing the moniker CALIPLUGMIKE, who sold Xanax tablets, among other illicit narcotics, including Adderall pills, mushrooms, LSD, and THC vaping cartridges. During their investigation, DEA Orange County agents learned that a parcel they had seized had been mailed by CALIPLUGMIKE and had originated from the Sacramento area. US Postal Inspectors reviewed surveillance images from the date and time the package had been mailed and confirmed that the individual who mailed the CALIPLUGMIKE parcel was TURRENTINE. The return name used on the Orange County parcel of interest bore the fictitious business name “CC101 Parts”.

B. CALIPLUGMIKE on the Empire Marketplace

25. CALIPLUGMIKE joined the Empire marketplace on May 24, 2019, offering to sell LSD, cocaine, Xanax pills, Adderall pills, psilocybin mushrooms, ecstasy, and marijuana products in various forms—including edibles, vape pens/cartridges, and marijuana buds in gram, ounce, and pound quantities—as well as compromised emails and passwords.

26. The Pretty Good Privacy (“PGP”) key provided by CALIPLUGMIKE was created on May 23, 2019, has the name “CaliPlugMike,” the fingerprint “94F2 571F 9756 4A8A 5C8A 6B8C C39C 5A67 EFB7 9E3F,” and the email “CaliPlugMike@secmail.pro” associated with it. As background, PGP is an encryption program that provides cryptographic privacy and authentication for data communication. PGP makes use of public-key encryption, in which one key is used to encrypt the data (the public key) and another key is used to decrypt it (the private key). This technology allows, for example, a dark-web drug vendor to communicate in an encrypted format by broadcasting his/her public key to customers who can then encrypt messages they want to send to the vendor.

27. As of April 4, 2020, CALIPLUGMIKE had 904 reviews on Empire Marketplace, with a customer service rating of 97.13% positive market feedback. Based on my training and

experience, as well as conversations with other law enforcement investigators knowledgeable of dark web investigations, I am aware that it is common for dark web vendors to make reference to their reviews and ratings from other dark web marketplaces as a means of gaining the customers' trust by showing to the customers that the vendor is an established and reputable seller. Under the "Terms and Conditions" on CALIPLUGMIKE's Empire Marketplace vendor page, CALIPLUGMIKE claimed to also be present on the Apollon and Versus Marketplaces, which are other dark web marketplace sites.³

C. CALIPLUGMIKE on the Apollon and DarkMarket Marketplaces

28. CALIPLUGMIKE was also present on the Apollon and DarkMarket marketplaces, on which he advertised similar—if not the same—items as he offered on his other dark market sites. The photographs and descriptions of the items were also similar, if not identical. CALIPLUGMIKE joined the Apollon marketplace on October 5, 2019, utilizing the same vendor name, CALIPLUGMIKE. By January 24, 2020, CALIPLUGMIKE had 223 sales with 100% positive feedback from customers.

29. CALIPLUGMIKE joined the DarkMarket marketplace in October 2019, again under the vendor name CALIPLUGMIKE. On January 13, 2020, CALIPLUGMIKE had completed two orders and had nine items listed for sale including LSD and various types and quantities of marijuana.

D. December 4, 2019 Undercover Purchase – 60 Counterfeit Xanax

30. On December 4, 2019, Sacramento undercover (UC) law enforcement agents ordered 60 Xanax bars (pills) from CALIPLUGMIKE on the Empire Marketplace.⁴

31. On December 5, 2019, CALIPLUGMIKE shipped a parcel in response to the order (UC PARCEL #1) via USPS Priority Mail, with tracking number 9114 9023 0722 4423

³ Although CALIPLUGMIKE appears to have operated on several marketplaces, all undercover purchases in this investigation were made on the Empire Marketplace.

⁴ For each of the undercover purchases described in this affidavit, unless otherwise noted, law enforcement agents executed the purchase using Bitcoin (or another cryptocurrency) and included a shipping address for a location controlled by law enforcement.

6189 07. USPS databases indicated that UC PARCEL #1 was mailed from a SSK located at the Perkins Post Office, 9500 Kiefer Blvd, Sacramento, and the sender had used a Visa debit card to pay for the postage.

32. On December 6, 2019, UC PARCEL #1 was delivered to the UC address agents had provided to CALIPLUGMIKE when they placed the order. The sender name and address on UC PARCEL #1's label was "CC101 Parts, 6435 Florin Perkins Rd, Sacramento, CA 95828."

33. On December 10, 2019, law enforcement opened UC PARCEL #1 and discovered two small plastic Ziploc style baggies containing green tablets marked with "S 90 3," consistent in appearance with counterfeit Xanax bars. The two small Ziploc baggies had been contained in a white, plastic pouch, inside a manila envelope. The white plastic pouch had an affixed label with typed writing, "Part # 18870-111." The total weight of the pills, including the two small plastic baggies, was approximately 17 grams, but field tests of several pills using a TruNarc device yielded inconclusive results for the presence of narcotics

34. On December 10, 2019, a Postal Inspector reviewed the SSK transactions associated with the purchase of the postage affixed to UC PARCEL #1 parcel and noted that TURRENTINE was the person who purchased the postage. Security camera footage from the time TURRENTINE purchased the postage showed him wearing a black "DGK" sweatshirt. His face was clearly visible.

35. On January 9, 2020, WRL Senior Forensic Chemist Son X. Hoang reported the results of his analysis of one of the suspected Xanax tablets obtained from UC PARCEL #1. The results revealed that the tablet consisted of flualprazolam.

E. Seizure of Parcel Containing Suspected Xanax Addressed to TURRENTINE

36. In December 2019, US Postal Inspectors conducted a check of USPS records and databases and learned that TURRENTINE was the listed recipient of numerous parcels originating from different states within the United States. On December 9, 2019, Postal Inspector Bauwens conducted a check of USPS records and discovered that TURRENTINE was the intended recipient of a parcel that had been mailed on December 10, 2019, and received its

first USPS scan at a processing plant in Nashua, New Hampshire (“NEW HAMPSHIRE PARCEL”). A check of USPS records indicated the postage on the NEW HAMPSHIRE PARCEL had been purchased via a third-party reseller of postage who solely accepts Bitcoin as payment (as explained above, given the pseudonymous nature of Bitcoin, dark web vendors trafficking in narcotics/narcotic proceeds through the US Mail often utilize Bitcoin to purchase postage to ship contraband, in order to avoid having their name attached to the purchase). The NEW HAMPSHIRE PARCEL was identified as a USPS Priority Mail parcel, with tracking number 9405 5368 9784 6196 9263 68.

37. On December 11, 2019, once the NEW HAMPSHIRE PARCEL had arrived in Sacramento, Inspector Bauwens took custody of it. It was addressed to “Jonathan TURRENTINE, 8620 Mellowoods Way, Sacramento, CA 95828-5027.” The return address on the NEW HAMPSHIRE PARCEL was “Jake Patterson, 1 Clocktower Pl, Apt 415, Nahua, NH 03060-3378.” On the same day, USPIS Task Force Officer Dave Moranz utilized his narcotics detection trained canine, “Farley,” who alerted to the presence of a narcotic odor from the NEW HAMPSHIRE PARCEL.

38. On December 16, 2019, the Honorable Deborah L. Barnes, United States Magistrate Judge for the Eastern District of California, authorized a search warrant for the NEW HAMPSHIRE PARCEL. At approximately 3:16PM, USPIS Inspectors Jason Bauwens, Trevor Covert, and DEA Special Agent Cindy Yamasaki executed the search warrant on the NEW HAMPSHIRE PARCEL. Inside the parcel, we discovered a number of green tablets with “S 90 3” imprinted on one side (consistent with counterfeit Xanax). The suspected Xanax was packaged in a white, padded pouch, inside a food saver bag, with the handwritten marking “1 K G.” Based on her training and experience, SA Yamasaki believed that “1 K G” indicated that the contents of the pouch contained 1,000 “green hulk” Xanax tablets. SA Yamasaki further believed that the sender of the NEW HAMPSHIRE PARCEL was one of TURRENTINE’s sources of supply for Xanax.⁵

⁵ CALIPLUGMIKE has made several references to his sources of supply on his vendor

39. On December 17, 2019, SA Yamasaki submitted the suspected counterfeit Xanax tablets (approximately 1,130 pills; 361.7 grams (gross)), seized from the NEW HAMPSHIRE PARCEL to the WRL. On January 9, 2020, WRL Senior Forensic Chemist Son X. Hoang reported that his analysis of one of the suspected Xanax tablets indicated that the suspected counterfeit tablet contained flualprazolam.

F. December 12, 2019 Undercover Purchase – 2 oz. marijuana

40. On December 12, 2019, agents in Sacramento placed an undercover order for two ounces of marijuana from CALIPLUGMIKE on the Empire Marketplace.

41. On December 13, 2019, CALIPLUGMIKE shipped a parcel in response to the order (UC PARCEL #2) via USPS Priority Mail, tracking number 9114 9023 0722 4598 0254 87. USPIS databases indicated that UC PARCEL #2 was mailed from a SSK located at the US Post Office, 7250 Elk Grove Florin Road, Sacramento.

42. On December 16, 2019, UC PARCEL #2 was delivered to the address agents had provided to CALIPLUGMIKE. The sender name and address on the UC PARCEL #2 was “CC101 Parts, 6435 Florin Perkins Rd., Sacramento, CA 95828.”

43. On December 20, 2019, investigators opened UC PARCEL #2 and discovered a large manila envelope, which contained two white, plastic sealed bags, each containing loose bulk marijuana. Each plastic sealed bag had an affixed label with typed writing: “Part # 18870-111.” USPIS Inspector Jason Bauwens placed the loose bulk marijuana in a plastic evidence

account pages on the Apollon, Empire, and DarkMarket Marketplaces. For example, after investigators had seized the NEWHAMPSHIRE PARCEL, CALIPLUGMIKE posted that the Xanax pills had been sourced by darkweb vendor PHARMAK11ING1. In addition, on or about January 13, 2020, CALIPLUGMIKE posted on his Apollon Marketplace “About Me” page that he was re-stocking certain items and even named the darkweb vendors that supplied him. He stated that he would be restocking his Xanax from darkweb vendor GREENBEANUSA and his supply of “Shrooms” from darkweb vendor GOLDENTEACHER. He also stated that people had complained about his previous supplies of Xanax from darkweb vendor HULKGOD because they were “under-dosed” (low in strength). CALIPLUGMIKE stated on his page that the customers should have checked HULKGOD’s reviews prior to purchasing Xanax from him and that his new source for Xanax would be GREENBEANUSA. Based on the foregoing, I believe that TURRENTINE obtains larger supplies of Xanax (and other narcotics) from other dark web vendors and, in turn, redistributes those Xanax tablets (and other narcotics) to numerous customers over the dark web under the vendor name CALIPLUGMIKE.

bag. The total weight of the marijuana, including the evidence bag, was approximately 64 grams. On January 9, 2020, SA Yamasaki submitted the suspected marijuana to the DEA Western Regional Laboratory for further testing and analysis and the results are pending.

44. On December 20, 2019, USPIS Inspector Bauwens reviewed the SSK transaction data associated with the purchase of the postage affixed to the UC PARCEL #2 parcel and observed that the person who purchased the postage was TURRENTINE. In the security camera footage, TURRENTINE's face was clearly visible and he was wearing a black "Raiders" sweatshirt.

G. December 19, 2019 Undercover Purchase – 4 Ecstasy Pills

45. On December 19, 2019, agents placed an order for four 250mg ecstasy pills from CALIPLUGMIKE on the Empire Marketplace.

46. On December 19, 2019, CALIPLUGMIKE shipped the parcel in response to this order (UC PARCEL #3) via USPS Priority Mail, tracking number 9114 9023 0722 4598 0257 08. USPIS databases indicated that UC PARCEL #3 was mailed from a SSK located at the US Post Office, 7250 Elk Grove Florin Road, Sacramento, CA 95829.

47. On December 20, 2019, UC PARCEL #3 was delivered to the undercover address. The sender name and address on UC PARCEL #3's label was "CC101 Parts, 6435 Florin Perkins Rd, Sacramento, CA 95828."

48. On December 26, 2019, law enforcement opened UC PARCEL #3 and discovered a manila envelope. Inside the envelope was a white plastic pouch, which contained a small plastic Ziploc-style baggie containing four green pills in the shape of Lego blocks. The white plastic pouch had an affixed label with typed writing, "Part # 18870-111." Law enforcement officers field tested the pills utilizing a TruNarc device that yielded inconclusive results for the presence of narcotics. The total weight of the suspected ecstasy pills, including the plastic baggie, was approximately 3 grams.

49. A postal inspector later reviewed the security footage of SSK transactions associated with the purchase of the postage affixed to the UC PARCEL #3 parcel and noted that

the person who purchased the postage was TURRENTINE. In the security camera footage, TURRENTINE's face was clearly visible and he was wearing the same black "Raiders" sweatshirt he wore when he had mailed UC PARCEL #2 on December 13, 2019.

50. On February 24, 2020, WRL Forensic Chemist Jonathan S. Park, reported the results of his analysis of one of the suspected ecstasy pills obtained from UC PARCEL #3. The results revealed that the tablet consisted of 3, 4-Methylenedioxymethamphetamine (MDMA or "Ecstasy").

H. December 19, 2019 Undercover Purchase – Six Viagra Pills

51. On December 19, 2019, agents placed an order for six Viagra pills from CALIPLUGMIKE on the Empire Marketplace.

52. On December 21, 2019, CALIPLUGMIKE shipped the parcel in response to this order (UC PARCEL #4) via USPS Priority Mail, tracking number 9114 9023 0722 4598 0256

92. USPS databases indicated that UC PARCEL #4 was mailed from a SSK located at the US Post Office, 7250 Elk Grove Florin Road, Sacramento.

53. On December 23, 2019, UC PARCEL #4 was delivered to the address agents had provided to CALIPLUGMIKE. The sender name and address on the UC PARCEL #4 label was "CC101 Parts, 6435 Florin Perkins Rd, Sacramento, CA 95828."

54. On December 30, 2019, investigators opened UC PARCEL #4 and again found an manila envelope. Inside the envelope, investigators found a white plastic pouch containing a partial blister pack containing six dark blue, oblong pills. The blister pack was labeled as "AUROBRA 100," which is a generic form of Viagra. The white pouch had an affixed label with typed writing, "Part #18870-111." The total weight of the Viagra pills, including the blister pack, was approximately 5 grams.

55. A postal inspector reviewed the surveillance footage of SSK transactions associated with UC PARCEL #4's affixed postage. The footage again showed TURRENTINE purchase the postage. TURRENTINE's face was clearly visible and he was wearing the same black "Raiders" sweatshirt that he wore when mailing UC PARCEL #2 and UC PARCEL #3.

I. January 1, 2020 Undercover Purchase – LSD Tablets

56. On January 1, 2020, agents ordered LSD tabs from CALIPLUGMIKE on the Empire Marketplace.

57. On January 3, 2020, CALIPLUGMIKE shipped the order (UC PARCEL #5) via USPS Priority Mail, tracking number 9114 9023 0722 4598 0262 24, again from the an SSK at the same US Post Office, 7250 Elk Grove Florin Road, Sacramento, CA 95829.

58. On January 4, 2020, agents received UC PARCEL #5 at the UC address. The sender name and address on the UC PARCEL #5 label was “CC101 Parts, 6435 Florin Perkins Rd, Sacramento, CA 95828.”

59. On January 8, 2020, investigators opened UC PARCEL #5 and found a manila envelope. The envelope contained a vacuum-sealed white plastic pouch, which contained a small plastic Ziploc style baggie containing multi-colored paper, divided into 25 small squares, which is consistent with LSD tabs. The white plastic pouch had an affixed label with typed writing, “Part # 18870-111.” Law enforcement officers field tested the suspected LSD tabs utilizing a TruNarc device that yielded inconclusive results for the presence of narcotics. The total weight of the suspected LSD tabs, including the small plastic baggie and vacuum-sealed plastic bag, was approximately 3 grams. On January 9, 2020, SA Yamasaki submitted the suspected LSD to the DEA Western Regional Laboratory for further testing and the results are pending.

60. A postal inspector reviewed the SSK transactions associated with the purchase of the postage affixed to the UC PARCEL #5 parcel and again saw that it was TURRENTINE who purchased the postage for UC PARCEL #5. TURRENTINE’s face was clearly visible and he was wearing a black “Raiders” sweatshirt (different from the Raiders sweatshirt he had worn when mailing UC PARCELS #2, #3, and #4.)

J. January 10, 2020 Undercover Purchase – 35 Counterfeit Adderall Pills

61. On January 10, 2020, agents ordered 35 Adderall pills from CALIPLUGMIKE on the Empire Marketplace.

62. On January 11, 2020, CALIPLUGMIKE shipped the order (UC PARCEL #6) via USPS Priority Mail, tracking number 9114 9023 0722 4770 7622 78. USPS databases indicated that UC PARCEL #6 was mailed from an SSK from the US Post Office, 7250 Elk Grove Florin Road.

63. On January 13, 2020, agents received UC PARCEL #6. The sender name and address on the UC PARCEL #6 label was again “CC101 Parts, 6435 Florin Perkins Rd, Sacramento, CA 95828.”

64. On January 27, 2020, law enforcement opened UC PARCEL #6 and found a manila envelope, containing a silver pouch. The pouch contained a small plastic Ziploc style baggie containing 35 round, orange pills, stamped with “AD” on one side, and “3 0” on the other side. The pills were consistent in appearance with counterfeit Adderall. The silver pouch had an affixed label with typed writing, “Part # 18870-111.” Investigators field-tested the suspected counterfeit Adderall tabs utilizing a TruNarc device which yielded a positive result for the presence of methamphetamine. The total weight of the suspected counterfeit Adderall pills, including the plastic baggie, was approximately 10 grams. On February 27, 2020, SA Yamasaki submitted the suspected counterfeit Adderall pills to the DEA Western Regional Laboratory for further testing and analysis and the results are pending.

65. A postal inspector subsequently reviewed footage of the SSK transactions associated with the postage affixed to UC PARCEL #6 and again observed that the person who purchased the postage was TURRENTINE. In the security camera footage, TURRENTINE’s face was again clearly visible, even though he had sunglasses on. He also had on the same black “Raiders” sweatshirt that he wore when mailing UC PARCEL #5.

K. January 10, 2020 Undercover Purchase – Email Password List

66. On January 10, 2020, agents ordered “1.4 billion email and password list” from CALIPLUGMIKE on the Empire Marketplace. The advertised price was \$1 and there were no associated shipping charges since the item was to be delivered digitally. CALIPLUGMIKE described the advertised item as follows: “(1) compiled from over 100 breaches into a simple

plain text file you can read; (2) Most people have changed their email password but most people use the same password across multiple sites; (3) You can use the email address and password to access any other sites like financial, social media, shopping sites, anything, etc.; (4) you can even look up your own email and see what password is out there linked to your email.

67. CALIPLUGMIKE sent electronically the links to the compromised emails and passwords to agents on or about January 13, 2020,

L. January 20, 2020 Undercover Purchases – Two Orders of Counterfeit Adderall Pills

68. On January 20, 2020, agents placed two orders for Adderall pills—one order for 30 pills and another for 18 pills—from CALIPLUGMIKE on the Empire Marketplace.

69. On January 22, 2020, CALIPLUGMIKE shipped the orders for the 35 Adderall pills (UC PARCEL #7) and 18 Adderall pills (UC PARCEL #8) via USPS Priority Mail, identified by tracking number 9114 9023 0722 4770 7638 62 (UC PARCEL #7) and tracking number 9114 9023 0722 4770 7639 16 (UC PARCEL #8). USPS databases indicated that both parcels were mailed from an SSK, at the same US Post Office, 7250 Elk Grove Florin Road.

70. On January 23, 2020, agents received UC PAREL #8, and on January 24, 2020, received UC PARCEL #7. The sender name and address on both parcels was “CC101 Parts, 6435 Florin Perkins Rd, Sacramento, CA 95828.”

71. On January 27, 2020, law enforcement opened UC PARCEL #7 and UC PARCEL #8. Both parcels contained a manila envelope with a silver pouch inside. Inside each of the silver pouches, investigators found small plastic Ziploc-style baggies containing round, orange pills, stamped with “AD” on one side, and “3 0” on the other side. These pills were consistent in appearance with counterfeit Adderall and identical to the pills contained in UC PARCEL #6. The silver pouches had an affixed label with typed writing, “Part # 18870-111.” Investigators field-tested the suspected counterfeit Adderall pills found in both parcels using a TruNarc device that yielded positive results for the presence of methamphetamine. The total weight of the pills found in UC PARCEL #7, including the small plastic baggie, was

approximately 9 grams. The total weight of the pills found in UC PARCEL #8, including the small plastic baggie, was approximately 6 grams.

72. On May 11, 2020, WRL Forensic Chemist Brittany Thomas reported the results of her analysis of sampling of the suspected counterfeit Adderall pills obtained from UC PARCEL #7 and UC PARCEL #8. The results revealed that the sample pills contained methamphetamine.

73. A postal inspector subsequently reviewed the SSK transactions associated with the postage affixed to UC PARCEL #7 and UC PARCEL #8, including security camera footage from the time of the purchase, and again observed that the person who purchased the postage was TURRENTINE. TURRENTINE's face was clearly visible, with sunglasses on, and he was wearing the same black "Raiders" sweatshirt that he wore when mailing UC PARCELS #2, #3, and #4.

M. January 30, 2020 Seizure of Parcel Containing Suspected LSD

74. On January 29, 2020, DEA SA Chris George spoke with Brad Hirsch, who represented himself as the attorney for "CC101," a cannabis dispensary located at 6435 Florin Perkins Road, Sacramento. Mr. Hirsch stated that, on that day, CC101 received a package that was marked "returned to sender" and that the sender information on the package was CC101's address. Mr. Hirsch stated that he had opened the package and discovered what he believed to be some form of illegal substance, possibly LSD. Mr. Hirsch stated that he did not believe the package had originated from CC101. Mr. Hirsch agreed to turn over the package and its contents to the DEA. Mr. Hirsch also stated that, on the same day, he received two letters from the United States Postal Inspection Service indicating that it was withholding two parcels with the return address belonging to CC101.

75. On January 30, 2020, Mr. Hirsch met with SA George and SA Ward and transferred custody of the package in question – a bubble-lined manila envelope addressed to "Hamman Aumi Rahman," 55 77th St, Apt 2F, Elmhurst, NY 11373, with sender information, "CC101 Parts, 6435 Florin Perkins Rd, Sacramento, CA 95828." The sender label, name, and

address were identical to those affixed to all eight of above described undercover purchases received from CALIPLUGMIKE, which TURRENTINE had mailed between December 4, 2019 and January 20, 2020. Inside the bubble-lined manila envelope was another manila envelope, a silver pouch with an affixed label with typed writing, “Part #18870-111,” a vacuum-sealed plastic bag, and a small plastic Ziploc style baggie containing 3 small squares of multi-colored paper. The multi-colored squares appeared consistent with LSD tabs. On January 31, 2020, SA George submitted the suspected LSD to the DEA Western Regional Laboratory for further testing and analysis and the results are pending.

76. Mr. Hirsch also provided SA George and SA Ward with copies of the two letters from the USPIS, addressed to CC101 Parts, 6435 Florin Perkins Rd, Sacramento. Both letters were dated January 22, 2020, and both advised CC101 Parts that packages that had been placed into the U.S. mail stream were being withheld from delivery due to belief that the contents of the items were hazardous, restricted, or perishable. One letter referenced an item sent to “Doug Urfali” at 8100 36th Ave N., Apt 201, Minneapolis, MN 55427 (Reference #: 20-NAC-06099-S). The second letter referenced an item sent to “Stephen Swanner” at 1027 Harris Lane, Wichita Falls, TX 76301 (Reference #: 20-NAC-06103-S).

77. Not long after interception of these three parcels, CALIPLUGMIKE posted on his vendor site that he had gone on vacation for “OPSEC” (operational security) reasons. An undercover agent sent CALIPLUGMIKE a direct message over Wickr, asking CALIPLUGMIKE if everything was okay. The undercover agent added that he/she wanted to “re-up on the addy” (read: purchase more Adderall). CALIPLUGMIKE responded, “im good, 1 pack [got] caught by x-ray, lame as hell, he just got a love note, nothing to worry about except Apollon exit scamming right now.”

78. Based on my training and experience, as well as the context, I believe that CALIPLUGMIKE advised the undercover agent that one of his parcels had been intercepted by the US Postal Service when he wrote that “1 pack [got] caught by x-ray.” I believe that CALIPLUGMIKE was possibly referring either to the parcel containing LSD that had been

returned to CC101, or the two other parcels intercepted by USPIS that had generated letters to CC101 (and which had therefore not made it to the intended recipients). I further believe that CALIPLUGMIKE was referring to these letters to CC101 about withholding delivery of the two intercepted parcels when he stated, “he just got a love note.” Finally, CALIPLUGMIKE assured the undercover agent that everything was fine except that the Apollon Marketplace was currently planning an “exit scam.”⁶

79. Following interception of these three parcels, CALIPLUGMIKE ceased using “CC101 Parts, 6435 Florin Perkins Road, Sacramento” as the sender information on parcels he mailed to his dark web customers. As described below in Paragraph 87, on February 10, 2020, TURRENTINE mailed 18 Priority Mail envelopes with sender address, “Alpine Supplies, 8112 Alpine Ave, Sacramento, CA 95826.” In addition, subsequent undercover purchases from CALIPLUGMIKE were received by law enforcement with the “Alpine Supplies” name and address listed as the sender.

N. December 10, 2019 to February 10, 2020 Surveillance of TURRENTINE

80. Between December 10, 2019 and February 10, 2020, law enforcement conducted no fewer than six surveillance operations targeting TURRENTINE. At the time, TURRENTINE resided at 8620 Mellowoods Way, Sacramento. On almost every occasion, law enforcement personnel observed TURRENTINE travel from his residence to a United States Post Office for the purpose of mailing items. The following paragraphs provide a summary of the surveillance.

81. On December 10, 2019, at approximately 12:00PM, agents observed TURRENTINE arrive at 8620 Mellowoods Way, Sacramento, in TURRENTINE VEHICLE #1, which he parked in the driveway. Agents observed TURRENTINE enter the residence.

82. On December 20, 2019, at approximately 9:30AM, agents observed TURRENTINE VEHICLE #1 parked in the driveway of 8620 Mellowoods Way. At

⁶ An “exit scam” is a transaction in which a vendor allows customers to place orders, for which the customers then transfer payment. The vendor then disappears (“exits”) from the market site in question without filling the orders. Vendors often commit exit scams when they believe they have been compromised or they no longer wish to do business on a particular dark site.

approximately 12:21PM, TURRENTINE exited the residence, departed in TURRENTINE VEHICLE #1, and drove to a Walmart.

83. At approximately 12:45PM, TURRENTINE departed the Walmart and arrived at the United States Post Office, 7250 Elk Grove Florin Road, Sacramento. TURRENTINE entered the post office and handed a white envelope to a postal clerk. TURRENTINE then exited the post office carrying a USPS mailing box. At approximately 1:03PM, TURRENTINE arrived back at 8620 Mellowoods Way.

84. On January 8, 2020, at approximately 1:55PM, TURRENTINE departed 8620 Mellowoods Way in TURRENTINE VEHICLE #1 and arrived at the Post Office, 7250 Elk Grove Florin Road, Sacramento. TURRENTINE drove up to a parcel drop box and deposited an envelope into the drop box.

85. On January 21, 2020, at approximately 12:43PM, TURRENTINE exited 8620 Mellowoods Way, carrying a white parcel. TURRENTINE departed in TURRENTINE VEHICLE #1 and drove to the post office on Elk Grove Florin Road. TURRENTINE entered the post office and deposited the parcel in a drop box. Agents were able to confirm that TURRENTINE mailed one box with USPS tracking number 9114 9023 0722 4770 7638 55, with sender label, "CC101 Parts, 6435 Florin Perkins Road, Sacramento, CA 95828," on that day. After mailing the parcel, TURRENTINE traveled to a Walmart located on Gerber Road and then to Natomas Auto Care, located at 1920 Terracina Drive #100, Sacramento. Surveillance units subsequently observed TURRENTINE standing behind the service desk inside Natomas Auto Care.

86. On February 3, 2020, at approximately 10:20AM, TURRENTINE exited 8620 Mellowoods Way with a dog and two clear plastic bags containing priority mail envelopes. TURRENTINE departed in TURRENTINE VEHICLE #1 and arrived at the Post Office at 7250 Elk Grove Florin Road. TURRENTINE entered the post office carrying the two bags of envelopes. TURRENTINE placed the priority mail envelopes from one bag into a mail drop box and then used the SSK to print shipping labels. TURRENTINE placed the shipping labels on the

envelopes contained in the second plastic bag and then deposited those envelopes into the drop box. Agents subsequently confirmed that TURRENTINE mailed 33 parcels during this visit. At approximately 10:40AM, TURRENTINE arrived back at 8620 Mellowoods Way.

87. On February 10, 2020, at approximately 10:02AM, TURRENTINE exited 8620 Mellowoods Way, carrying two bags, and departed in TURRENTINE VEHICLE #1. At approximately 10:06AM, TURRENTINE arrived at the Post Office at 7250 Elk Grove Florin Road. TURRENTINE placed eighteen Priority Mail envelopes into a drop box inside the post office. TURRENTINE exited the post office carrying two packages and departed, arriving back at the Mellowoods residence at approximately 10:15AM. Agents were able to confirm that TURRENTINE mailed 18 packages with the same sender address, “Alpine Supplies, 8112 Alpine Ave, Sacramento, CA 95826,” during this visit.

88. A Google search indicates that the address 8112 Alpine Avenue, Sacramento, is associated with “Vibe by California,” which advertises itself as a “vertically integrated cannabis company/cannabis retailer.” A Google search also indicates that 6435 Florin Perkins Road, Sacramento, which CALIPLUGMIKE previously used as his sender address prior to the interception of the three parcels in January 2020, is associated with “CC101,” a medical and recreational marijuana dispensary. There is no indication that TURRENTINE has any affiliation with “Vibe of California” or “CC101” and appears to be using these addresses without the permission or knowledge of the businesses.

O. February 29, 2020 Undercover Purchase – 90 Counterfeit Adderall Pills

89. On February 29, 2020, agents placed an order for 90 Adderall pills from CALIPLUGMIKE on the Empire Marketplace.

90. On March 2, 2020, CALIPLUGMIKE shipped the order (UC PARCEL #9) via USPS Priority Mail, tracking number 9114 9023 0722 4769 3537 91, using an SSK located at the US Post Office, 7250 Elk Grove Florin Road, Sacramento.

91. On March 3, 2020, agents received UC PARCEL #9. The sender name and address on the UC PARCEL #9 label was “Alpine Supplies, 8112 Alpine Ave, Sacramento, CA

95829.”

92. On March 4, 2020, law enforcement opened UC PARCEL #9 and discovered a manila envelope containing a white pouch. The pouch contained three small plastic Ziploc-style baggies containing approximately 90 round, orange pills, stamped with “3 0” on one side, and “dp” on the other side. The pills were consistent in appearance with counterfeit Adderall. The white pouch had an affixed label with typed writing, “Order # 57948.” Law enforcement officers field tested the suspected counterfeit Adderall pills using a TruNarc device that yielded a positive result for the presence of methamphetamine. The total weight of the suspected counterfeit Adderall pills, including the plastic packaging, was approximately 35 grams.

93. On April 10, 2020, WRL Forensic Chemist Thomas N. Teadt reported that his analysis of one of the suspected counterfeit Adderall pills indicated that the pill weighed approximately 0.403 grams and contained methamphetamine. The total weight of the 90 pills was approximately 37.703 net grams.

94. A postal inspector reviewed the SSK transactions associated with the purchase of the postage affixed to the UC PARCEL #9, including security camera footage, and observed that the person who purchased the postage was TURRENTINE. TURRENTINE’s face was clearly visible and he was wearing the same black “Raiders” sweatshirt that he wore when mailing UC PARCELS ## 2, 3, 4, 7 and 8.

P. March 2, 2020 Undercover Purchase – 40 Counterfeit Adderall Pills

95. On March 2, 2020, agents ordered 40 Adderall pills from CALIPLUGMIKE on the Empire Marketplace.

96. On March 3, 2020, CALIPLUGMIKE shipped the order (UC PARCEL #10) via USPS Priority Mail, tracking number 9114 9023 0722 4617 0927 04, from a SSK at a US Post Office, 7250 Elk Grove Florin Road, Sacramento, CA 95829.

97. On March 6, 2020, agents received UC PARCEL #10. The sender name and address on the UC PARCEL #10 label was “House of Organics, 8848 Fruitridge Rd, Sacramento, CA 95826.” A Google search indicates that “House of Organics” is a cannabis

dispensary. There is no indication that TURRENTINE is affiliated with House of Organics.

98. On March 10, 2020, law enforcement opened UC PARCEL #10. As usual, it contained a manila envelope, which contained a silver pouch. Inside the pouch were two small plastic Ziploc-style baggies containing approximately 40 round, orange pills, stamped with “3 0” on one side, and “AD” on the other. The pills were consistent in appearance with counterfeit Adderall. The silver pouch had an affixed label with typed writing, “House of Organics Order # 11389.” Law enforcement officers field tested the suspected counterfeit Adderall pills utilizing a TruNarc device which yielded a positive result for the precursor Barium sulfate. The total weight of the suspected counterfeit Adderall pills, including the plastic baggies, was approximately 17 grams.

99. On May 5, 2020, WRL Forensic Chemist KeiSharra Eldridge reported the results of her analysis of a sample of the suspected counterfeit Adderall pills obtained from UC PARCEL #10. The results revealed that the sample pills contained amphetamine and caffeine.

100. A postal inspector reviewed the SSK transactions associated with the purchase of the postage affixed to the UC PARCEL #10, including security camera footage, and observed that the person who purchased the postage was TURRENTINE. TURRENTINE’s face was clearly visible and he was wearing the same black “Raiders” sweatshirt that he wore when mailing UC PARCELS # 5 and # 6.

Q. Undercover Purchase from Dark Web Vendor CALIPLUGMIKE on March 9, 2020 Corresponding Surveillance of TURRENTINE Mailing the UC Purchase on March 10, 2020, and Identification of TURRENTINE’s New Residence, 9161 Tuolumne Drive, Sacramento, CA

101. On March 9, 2020, agents ordered 30 Adderall pills from CALIPLUGMIKE on the Empire Marketplace.

102. On March 10, 2020, at approximately 8:55AM, law enforcement personnel established surveillance at 8620 Mellowoods Way and at the US Post Office at 7250 Elk Grove Florin Blvd. At approximately 9:54AM, USPIS TFO Dave Moranz observed TURRENTINE arrive at the post office in his dark green TURRENTINE VEHICLE #1. TFO Moranz noted that

TURRENTINE was wearing jeans and a black sweatshirt. TFO Moranz observed TURRENTINE use the SSK located inside the post office to purchase postage and subsequently drop several USPS Priority Mail envelopes into a mailbox. A subsequent review of SSK images showed TURRENTINE purchasing postage for the parcels and wearing the same black Raiders sweatshirt that he wore when mailing UC PARCELS #5, #6, and #10. TFO Moranz saw TURRENTINE leave the post office at approximately 9:59AM.

103. Agents observed TURRENTINE stop briefly at a small park near the 8620 Mellowoods Way residence with a small dog. TURRENTINE then traveled to the residence located at 9161 Tuolumne Drive, Sacramento, arriving at approximately 10:31AM. Agents observed TURRENTINE park TURRENTINE VEHICLE #1 on the street in front of the residence and enter the residence with the small dog. At approximately 11:25AM, agents observed TURRENTINE exit the residence, place items into a trash can located on the street, relocate the trash can to the side of the residence, and depart in TURRENTINE VEHICLE #1.

104. Later that day, agents retrieved and photographed all the Priority Mail envelopes that TURRENTINE had deposited in the mailbox. In total, TURRENTINE had deposited nine envelopes, including the parcel related to the UC purchase on March 9, 2020 (UC PARCEL #11), which was identified by tracking number 9114 9023 0722 4617 0921 55. The sender information on all nine parcels was "House of Organics, 8848 Fruitridge Rd, Sacramento, CA 95826." The other eight parcels were destined for different addresses in Ohio, Utah, North Carolina, Tennessee, California, and Pennsylvania. Law enforcement placed the remaining eight envelopes back into the mail stream.

105. On March 10, 2020, law enforcement opened UC PARCEL #11 and found a manila envelope containing a silver pouch. Inside the pouch there was a small plastic Ziploc-style baggie containing approximately 30 round, orange pills, stamped with "3 0" on one side, and "AD" on the other side, consistent in appearance with counterfeit Adderall. The silver pouch had an affixed label with typed writing, "House of Organics Order # 11389." Agents field tested the suspected counterfeit Adderall pills utilizing a TruNarc device which yielded a

positive result for the precursor Barium sulfate. The total weight of the suspected counterfeit Adderall pills, including the plastic baggies, was approximately 13 grams.

106. On April 20, 2020, WRL Forensic Thomas N. Teadt reported the results of his analysis of three of the suspected Xanax tablets. The results revealed that of the 30 pills submitted, two of the pills were marked with “d p” on one side and “AD” on the other side. The remaining 28 pills were marked with “3 0” on one side and “AD” on the other side. The two pills stamped with “d p” weighed approximately 0.806 grams and contained methamphetamine. A single pill of the remaining 28 pills stamped “AD” was analyzed, which weighed approximately 0.477 grams and consisted of amphetamine and caffeine. The total weight of the 30 pills was approximately 12.283 net grams.

R. Surveillance of TURRENTINE on March 17, 2020

107. On March 17, 2020, at approximately 7:01AM, SA Yamasaki observed TURRENTINE VEHICLE #1 parked across the street, near the residence of 9161 Tuolumne Drive, Sacramento. At approximately 9:37AM, SA Yamasaki observed TURRENTINE walk from the direction of the residence with a small dog, carrying a plastic grocery bag. TURRENTINE departed the area and arrived at the US Post Office, 7250 Elk Grove Florin Road at approximately 9:49AM. SA Yamasaki observed TURRENTINE carry the plastic grocery bag inside the post office and walk to a SSK to purchase postage. She observed that the plastic grocery bag contained numerous Priority Mail envelopes and that TURRENTINE utilized a card to pay for his transaction. Upon completing his transaction, TURRENTINE threw his receipts in the trash can and walked to a counter located directly behind the kiosk. Moments later, SA Yamasaki observed TURRENTINE place the Priority Mail envelopes into a mailbox and exit the post office.

108. SA Yamasaki retrieved two receipts that TURRENTINE threw in the trash can and observed that TURRENTINE purchased postage for seven parcels and used a US debit card to pay for the postage. With the assistance of US Postal Inspectors, SA Yamasaki photographed all of the Priority Mail envelopes that TURRENTINE deposited in the mailbox. She confirmed

that TURRENTINE deposited a total of seven envelopes, all of which had a sender label marked, “House of Organics, 8848 Fruitridge Rd, Sacramento, CA 95826.” The seven parcels were destined for different addresses located in New Jersey, Ohio, Colorado, New York, California, and Pennsylvania. Law enforcement placed the 7 envelopes back into the mail stream.

S. Money Laundering Activity by TURRENTINE

109. Based on my training and experience investigating individuals who sell drugs on the darknet, and who accept cryptocurrency, including bitcoin, there is a need to cash out their cryptocurrency for fiat currency. The most common way to facilitate this is by using a cryptocurrency exchange company.

110. During this investigation, investigators obtained records for a CEX.IO Limited account owned by TURRENTINE. CEX.IO Limited is a cryptocurrency exchange company located in the United Kingdom. CEX.IO Limited offers their account holders the option to convert bitcoin into fiat and, in turn, transfer the fiat to card payments and bank transfers. According to CEX.IO Limited records, TURRENTINE opened an account in or about May 2017.⁷ TURRENTINE provided a debit card number ending in 4296 to CEX.IO to transfer the fiat from the sale of his Bitcoin onto his debit card ending in 4296.⁸

111. During the investigation, investigators obtained records from The Bancorp Bank (“Bancorp”) for the debit card number ending in 4296. According to Bancorp records, in about August 2018, TURRENTINE opened a Chime consumer debit card and he was assigned this debit card number. Unlike a traditional bank account, a Chime consumer debit card account allows individuals and companies to transfer money directly onto a debit card.

112. As previously described in this affidavit, all undercover purchases for drugs from CALIPLUGMIKE were paid for with Bitcoin. Based on a review of financial records associated to TURRENTINE and the physical surveillance of him, investigators believe that the only source

⁷ TURRENTINE’s CEX.IO Limited account only had a handful of transactions between on or about May 2017 and October 2019.

⁸ It is unclear from the records that were provided by CEX.IO Limited when this occurred.

of TURRENTINE's Bitcoin is from the sale of drugs on the darknet.

113. Based on the undercover purchases executed in this investigation and a review of financial records obtained from CEX.IO Limited and Bancorp, there is probable cause to believe that TURRENTINE is using proceeds from the sale of drugs on the dark web to pay for the shipping costs at various U.S. Post Office kiosks, in violation of 18 U.S.C. §§ 1956(a)(1)(A)(i). For example, as described above, on January 20, 2020, Sacramento law enforcement placed two orders of Adderall pills from CALIPLUGMIKE on the Empire Marketplace. TURRENTINE shipped the parcels containing these orders of Adderall pills (UC PARCELS #7 and #8) via USPS Priority Mail, costing \$7.35 each. USPIS database records indicate that TURRENTINE paid the shipping costs using his debt card ending in 4296.⁹ Likewise, as described above, on March 9, 2020, agents ordered 30 Adderall pills from CALIPLUGMIKE on the Empire Marketplace. The next day, agents personally observed TURRENTINE mail the parcel containing that order (UC PARCEL #11), which he shipped via Priority Mail, at a cost of \$7.75. Again, TURRENTINE used his debit card ending in 4296, thereby using the proceeds of illicit narcotics sales to pay for postage.¹⁰

T. Investigation of CALIPLUGMIKE by DEA Orange County

114. In approximately December 2019, the NCIDE Task Force learned that DEA, USPIS, and HSI in Orange County, as well as the Costa Mesa Police Department (hereinafter referred to as the "Orange County Agencies"), were investigating the death of an 18-year old who they believe committed suicide after taking counterfeit Xanax purchased on the dark web. After analyzing the victim's dark net market accounts, investigators learned that the victim frequently ordered narcotics on dark net marketplaces. Investigators learned that the victim had

⁹ According to Bancorp records, 100% of the funds on debit card ending in 4296 at the time UC PARCEL #'s 7 and 8 were paid for with funds that had been transferred from TURRENTINE's CEX.IO Limited account.

¹⁰ At the time agents personally observed TURRENTINE mail UC PARCEL #11, he also mailed eight additional parcels along with UC PARCEL #11. According to Bancorp records, 100% of the funds on the debit card ending in 4296 at the time Turrentine paid to ship UC PARCEL #11 and the other eight parcels had been paid for with funds transferred from TURRENTINE's CEX.IO Limited account.

ordered a package from a vendor with moniker “CALIPLUGMIKE” on the Empire Marketplace. The package had been mailed from Sacramento.

115. On December 4, 2019, the Orange County Agencies purchased 41 Xanax pills from CALIPLUGMIKE for 0.01274509 Bitcoin (approximately \$2 per pill, plus shipping costs). On December 9, 2019, the agents opened the parcel containing approximately 41 green pills, with “S093” imprinted on them. The suspected Xanax was packaged identically to the parcels the NCIDE Task Force agents had received from their orders to CALIPLUGMIKE, including packaging labeled “Part # 18870-111,” with the return address, “CC101 Parts, 6435 Florin Perkins Rd, Sacramento, CA 95828.”

116. On January 14, 2020, the Orange County Agencies ordered from CALIPLUGMIKE 12 Adderall pills, for 0.01210994 Bitcoin (approximately \$8 per pill, plus shipping costs), 4,125 microgram LSD tabs, for 0.00435081 Bitcoin (approximately \$7 per tab, plus shipping costs), and two grams of “fishscale” cocaine, for 0.01465535 Bitcoin (approximately \$59 per gram, plus shipping costs). On January 21, 2020, agents opened the parcel from CALIPLUGMIKE containing the suspected Adderall pills, LSD, and cocaine. Again, the sender information on the parcel was “CC101 Parts, 6435 Florin Perkins Road, Sacramento, CA 95828” and an inner envelope was labeled “Part #18870-111.” On March 26, 2020, Southwest Laboratory Senior Forensic Chemist Dean A. Kirby reported the results of his analysis of the suspected LSD obtained from the UC purchase. The results revealed that the blotter paper consisted of Lysergic Acid Diethylamide (LSD).

117. On February 14, 2020, the Orange County Agencies purchased 70 Xanax pills, 9 Adderall pills, 1 gram of “fishscale” cocaine, 1,350 mg Orange CP ecstasy, and 2,125 microgram LSD tabs, using Bitcoin as payment. On February 18, 2020, agents opened the parcel sent by CALIPLUGMIKE containing the above described purchase. This parcel listed the return sender as “Alpine Supplies, 8112 Alpine Ave, Sacramento, CA 95826,” and the interior packaging was labeled “Order # 57948.”

U. CALIPLUGMIKE Exits the Empire Marketplace

118. Beginning on or about April 4, 2020, feedback on CALIPLUGMIKE's Empire vendor page indicated that CALIPLUGMIKE had performed an exit scam. Numerous customers posted comments that CALIPLUGMIKE had taken their money and had not provided the promised products. CALIPLUGMIKE also changed his "About" information to read only, "GOODBYE," indicating that he had in fact left the Empire Marketplace. Around this same time, there were numerous posts on dark web forums discussing CALIPLUGMIKE's exiting the Empire Marketplace.

119. On or about April 14, 2020, an undercover agent sent CALIPLUGMIKE a direct message over Wickr (the agent had CALIPLUGMIKE's Wickr contact information from their course of transactions), asking CALIPLUGMIKE if he was starting a new sales account, as the undercover agent wanted to purchase more Adderall. CALIPLUGMIKE responded "DD here only," which the agent understood to mean that he was engaging only in "direct deals" over Wickr (and likely only with customers with whom he had done business in the past), and that he was not selling products on dark web marketplaces. The undercover agent responded that he/she had heard that CALIPLUGMIKE had left Empire Marketplace, but CALIPLUGMIKE did not respond.

120. Following CALIPLUGMIKE's exit from Empire Marketplace, he appeared to cease transacting business, until investigators picked up another lead on him in November 2020.

V. CALIPLUGMIKE identified as DATCUBENSISBOY on Dark Market Marketplace

121. In November 2020, Postal Inspector Bauwens identified a suspicious parcel with tracking number 9405536897846258720873, addressed to A.K.¹¹, at an address in Iowa. The sender name and address on the parcel was "Morgan Ebay Store, PO Box 292172, Sacramento, California." Inspector Bauwens contacted Iowa-based Postal Inspector Bryce Husak and requested that Inspector Husak conduct a "knock and talk" at the delivery address, in an attempt to ascertain the contents of the package and identify the sender of the parcel.

¹¹ These are the individual's initials which are being used to protect his identity.

122. On November 5, 2020, Inspector Husak and Dubuque County Sheriff Investigator Jeremy Slight interviewed A.K. at his residence. A.K.'s uncle and guardian, N.K., was present during the interview. Inspector Husak informed A.K. that the interview was voluntary and could be terminated at any time. A.K. gave Inspector Husak consent to open the parcel, which contained approximately one ounce of what appeared to be marijuana. A.K. stated that he had ordered this parcel, as well as previous parcels, from the "Dark Market" marketplace, from a vendor using the moniker DATCUBENSISBOY. A.K. showed Inspector Husak his history of dark web orders, including several orders from DATCUBENSISBOY.

W. November 9, 2020 Undercover Purchase from Dark Web Vendor DATCUBENSISBOY

123. On November 9, 2020, Sacramento-based agents went on to the Dark Market Marketplace, and placed an order of fifteen 10ml syringes containing Golden Teacher mushroom spores, along with sterile needles, from DATCUBENSISBOY.

124. On November 10, 2020, DATCUBENSISBOY shipped the parcel (UC PARCEL #12) via United States Postal Service (USPS) Priority Mail, tracking number 9405 5368 9784 6289 4264 85, from the US Post Office, 7250 Elk Grove Florin Road, Sacramento, CA 95829.

125. On November 13, 2020, agents received UC PARCEL #12. The sender information on UC PARCEL #12 label was "MORGAN EBAY STORE, PO Box 292172, Sacramento, CA 95829" (the same as the sender information on the package sent to A.K.).

126. On November 23, 2020, law enforcement opened UC PARCEL #12 and discovered multiple padded manila envelopes, multiple USPS small boxes, and a sealed, silver foil pouch. Affixed to the outside of the foil pouch, was a sticker with the words, "Morgan eBay Store Order #428095." The packaging and labeling on the foil pouch were similar to and consistent with the other packages agents had received from TURRENTINE/CALIPLUGMIKE during the earlier investigation. Inside the foil pouch, agents found 15 syringes containing a clear liquid with small, black spore-like particles floating in the liquid. Also included in the foil pouch were numerous alcohol wipes and 18-gauge needle tips. The liquid filled syringes,

including their packaging, weighed 283 grams.

X. Identification of parcels mailed by DATCUBENSISBOY on November 19, 2020

127. On November 21, 2020, Postal Inspector Bauwens identified four suspicious parcels mailed from the U.S. Post Office, 7250 Elk Grove Florin Road, Sacramento. The four parcels were scanned as “accept or pickup” by post office staff on November 19, 2020, at 1:27PM. The four parcels bore the fictitious sender name “MORGAN EBAY STORE, PO Box 292172, Sacramento, CA 95829,” the same name used by dark web vendor DATCUBENSISBOY. The four parcels were destined for Columbia, MD (USPS tracking number 9400 1368 9784 6321 2606 85); Hahira, GA (USPS tracking number 9400 1368 9784, 6321 2612 48); San Diego, CA (USPS Tracking number 9400 1368 9784 6321 2618 35); and Cincinnati, OH (USPS tracking number 9400 1368 9784 6321 2621 39).

128. SA Bauwens reviewed security camera video from the U.S. Post Office, 7250 Elk Grove Florin Road, from the time the packages were shipped, and observed TURRENTINE mailing parcels similar in appearance to the four parcels, at a collection box inside the post office. TURRENTINE’s face is visible in the video and he is wearing a Raiders sweatshirt that is identical in appearance to the sweatshirt he wore when mailing previous undercover parcels.

Y. November 23, 2020 Undercover Purchase from Dark Web Vendor DATCUBENSISBOY

129. On November 23, 2020, agents ordered ten Golden Teacher mushroom spore prints from DATCUBENSISBOY on the Dark Market Marketplace.

130. On November 24, 2020, DATCUBENSISBOY shipped the parcel containing this order (UC PARCEL #13) via Priority Mail, tracking number 9405 5368 9784 6337 3331 09, from the US Post Office, 7250 Elk Grove Florin Road, Sacramento.

131. On November 27, 2020, agents received UC PARCEL #13. The sender information on UC PARCEL #13 label was “MORGAN EBAY STORE, PO Box 292172, Sacramento, CA 95829.”

132. On December 14, 2020, law enforcement opened UC PARCEL #13 and

discovered a single padded manila envelope, affixed with a sticker with the words, “Morgan eBay Store Order #428095.” Inside the manila envelope was a sealed gray pouch with an identical sticker affixed to the outside. Inside the gray pouch were numerous alcohol wipes and 10 squares of aluminum foil, each of which contained a black, flaky substance, presumed to be the advertised mushroom prints. The total weight of the mushroom prints, including the foil packaging, was 6 grams.

133. A postal inspector subsequently reviewed video at the US Post Office, 7250 Elk Grove Florin Blvd., from the day and time UC PARCEL #13 was shipped, and determined that approximately two hours before UC PARCEL #13 was scanned as “accepted” by the post office staff, a male, wearing a face mask, entered the post office carrying a USPS envelope which appears similar to UC PARCEL #13. After entering the post office, the male exited the view of the camera and emerged again a short time later before departing the post office empty-handed. While the male’s face is never clearly visible, he bears a strong resemblance to TURRENTINE in stature, appearance, and movement.

Z. Closure of the Dark Market Marketplace in January 2021

134. In January 2021, law enforcement successfully shut down the Dark Market Marketplace, which hosted hundreds of thousands of users and facilitated hundreds of thousands of illegal transactions, including those of DATCUBENSISBOY. As a result, law enforcement is unable to make further undercover purchases from DATCUBENSISBOY at this time. Additionally, if TURRENTINE continues his illicit sales on other dark web marketplaces, it is likely he will likely change his moniker, as he did when he ceased doing business under the moniker CALIPLUGMIKE, to avoid detection by law enforcement. As of this date, law enforcement has been unsuccessful in ascertaining whether TURRENTINE has re-established himself as a vendor on another dark web marketplace and, if so, what his new moniker is.

AA. Recent Surveillance of TURRENTINE at the TARGET PROPERTY (9161 Tuolumne Drive, Sacramento, California) and Evidence Expected to Seized at the TARGET PROPERTY

135. On August 19, 2021, agents from one of the FBI’s surveillance teams established

surveillance of the TARGET PROPERTY. Upon initiating surveillance of the TARGET PROPERTY at approximately 1:43PM, agents observed a Hyundai SUV bearing California license plate number 8UXX035 and VIN KM8JU3AC1CU441924, registered to S.T. (TURRENTINE VEHICLE #2) parked in the driveway. Shortly after initiating surveillance at the TARGET PROPERTY, TURRENTINE was observed exiting the TARGET PROPERTY and accessed TURRENTINE VEHICLE #2 from the passenger side of the vehicle. TURRENTINE appeared to go through the glove box of TURRENTINE VEHICLE #2 and then he returned inside of the TARGET PROPERTY.

136. On September 2, 2021, agents from one of FBI's surveillance teams established surveillance of the TARGET PROPERTY. Upon initiating surveillance of the TARGET PROPERTY, at 8:10AM, agents observed TURRENTINE walking a dog and subsequently walking towards the front door of the TARGET PROPERTY. At 2:08PM, agents observed TURRENTINE walkout of the TARGET PROPERTY and enter TURRENTINE VEHICLE #1 and depart the residence. At 2:10PM, agents observed TURRENTINE arrive at La Riveria Market and Spirits located at 9331 La Riveria Dr., Sacramento, CA, and walked inside. At 2:13PM, agents observed TURRENTINE exit the store, return to TURRENTINE VEHICLE #1, and depart the store location. At 2:15PM, agents observed TURRENTINE return to the TARGET PROPERTY. TURRENTINE parked TURRENTINE VEHICLE #1 on the street in front of the TARGET PROPERTY. Agents observed TURRENTINE exit TURRENTINE VEHICLE #1 and walk towards the TARGET PROPERTY carrying a black bag in his hands.

137. As set forth above in Paragraph 134, law enforcement has not been successful in identifying TURRENTINE's new moniker due to the DarkMarket Marketplace being successfully shut down by law enforcement. Because of this, it is unknown if TURRENTINE is still distributing illegal narcotics on the dark web, in violation of Title 21 U.S.C. §§ 841(a)(1) and 846, trafficking in counter goods and services, in violation of Title 18 U.S.C. § 2320 (a)(4), and laundering the criminal derived proceeds, in violation of Title 18 U.S.C. §§ 1956 (a)(1)(A)(i). However, there is probable cause to believe the following evidence will be seized at

the TARGET PROPERTY, TURRENTINE VEHICLE #1, TURRENTINE VEHICLE #2, and TURRENTINE's person, including but not limited to:

- a) Documents, records or information relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of controlled substances;
- b) Documents, records or information relating to the purchase, sale, tracking, delivery or distribution of postage or express mail consignment;
- c) Documents, records or information relating to the transfer, purchase, sale or disposition of virtual currency;
- d) Documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services;
- e) Documents, records, or information relating to email accounts used in furtherance of these offenses;
- f) Efforts to avoid detection by law enforcement;
- g) Records relating to indicia of occupancy, residency, and ownership or use of the TARGET PROPERTY, TURRENTINE VEHICLE #1, TURRENTINE VEHICLE #2, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase or lease agreements, identification documents, and keys; and
- h) Bank records, checks, credit card bills, account information, safe deposit box information and other financial records.

138. In my training and experience, persons engaged in drug trafficking, trafficking in counterfeit goods and services, and laundering of the criminal derived proceeds often maintain such records for long periods of time, particularly when they are involved in ongoing criminal conduct over a long period of time. Based on my experience and review of *United States v Greany*, 929 F.2d 523 (9th Cir. 1991), the Ninth Circuit and other courts have held that, where there is an ongoing criminal business or where the evidence is of a nature that would be kept long after the criminal activity has ceased, the passage of long periods of time will not make the evidence supporting the issuance of a warrant stale.

139. There are many reasons why persons involved persons engaged in drug trafficking, trafficking in counterfeit goods and services, and laundering of the criminal derived proceeds, such as TURRENTINE, maintain evidence for long periods of time. The evidence may be innocuous at first glance (e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, utility records, ownership/rental records, financial records, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but have significance and relevance when considered in light of other evidence. The criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed any computer-related evidence, but which may be retrievable by a trained forensic computer expert. Based on the facts presented, TURRENTINE has used an electronic device(s) to further his crimes.

140. Based on the forgoing, there is probable cause to believe evidence associated to TURRENTINE's drug trafficking, trafficking in counterfeit goods and services, and the laundering of the criminally derived proceeds will be located at the TARGET PROPERTY, TURRENTINE VEHICLE #1, TURRENTINE VEHICLE #2, and TURRENTINE's person.

VI. METHODS AND MEANS OF USING THE UNITED STATES MAIL

141. Based on my experience, training, and discussions with other law enforcement officers experienced in drug investigations, I know that certain indicators exist when persons use the United States Mail to ship controlled substances from one location to another. Indicators for parcels that contain controlled substances and/or proceeds from controlled substances include, but are not limited to, the following:

- a) It is common practice for shippers of the controlled substances to use Express Mail and Priority Mail because the drugs arrive at the destination more quickly and on a predictable date. Express Mail and Priority Mail, when paired with a special service such as delivery confirmation, allow traffickers to monitor the progress of the shipment of

controlled substances. Traffickers pay for the benefit of being able to confirm the delivery of the parcel by checking the Postal Service Internet website and/or calling the local post office.

b) Packages containing controlled substances or proceeds have, in many instances, a fictitious return address, incomplete return address, no return address, a return address that is the same as the addressee address, or a return address that does not match the place from which the parcel was mailed. These packages are also sometimes addressed to or from a commercial mail receiving agency (*e.g.*, Mail Boxes Etc.). A shipper may also mail the parcel containing controlled substances from an area different from the return address on the parcel because: (1) the return address is fictitious or (2) the shipper is attempting to conceal the actual location from which the parcel was mailed. These practices are used by narcotics traffickers to hide from law enforcement officials the true identity of the persons shipping and/or receiving the controlled substances or proceeds.

c) Individuals involved in the trafficking of controlled substances through the United States Mail will send and receive Express or Priority mailings on a more frequent basis than a normal postal customer. Drug traffickers use Express Mail and Priority Mail at a higher rate due to their frequent exchanges of controlled substances and the proceeds from the sale of these controlled substances.

d) In order to conceal the distinctive smell of controlled substances from narcotics detection dogs, these packages tend to be wrapped excessively in bubble-pack and wrapping plastic, and are sometimes sealed with the use of tape around all seams. In addition, the parcels often contain other smaller parcels which are carefully sealed to prevent the escape of odors. Perfumes, coffee, dryer sheets, tobacco, or other substances with strong odors are also sometimes used to mask the odor of the controlled substances being shipped. Drug traffickers often use heat/vacuum sealed plastic bags, and/or re-sealed cans in an attempt to prevent the escape of odors.

e) California is typically a source state for drugs, especially marijuana. It is

common for individuals in California to manufacture marijuana, to mail parcels containing narcotics to other states and then receive mail parcels containing cash payments in return.

142. Based on my training and experience and discussions with other law enforcement officers, I know that parcels shipped by drug traffickers sometimes contain information and documentation related to the sales and distribution of controlled substances. The documentation can include, but is not limited to, information and instructions on the breakdown and distribution of the controlled substances at the destination; information on the use and effects of the various controlled substances; information about the actual sender; pay/owe sheets; and information and instructions for ordering future controlled substances.

143. Drug traffickers who use the United States Mail and other carriers as a means of distributing controlled substances, paraphernalia, and proceeds, and as a means of communicating with co-conspirators often include the following in parcels relating to their trafficking activity, all of which are evidence, fruits, proceeds, and/or instrumentalities of violations of 21 U.S.C. §§ 841(a)(1), 843(b), and 846:

- a) Controlled substances, including heroin, cocaine, methamphetamine, and marijuana.
- b) Packaging, baggies, and cutting agents, including items used to conceal the odor of narcotics, such as perfumes, coffee, dryer sheets, tobacco, or other substances with a strong odor.
- c) Records reflecting the mailing or receipt of packages through Express Mail, Priority Mail, Federal Express, UPS or any other common carrier.
- d) United States and foreign currency, securities, precious metals, jewelry, stocks, bonds, in amounts exceeding \$500, including financial records related to the laundering of illicitly obtained monies and/or other forms of assets, including United States currency acquired through the sales, trafficking, or distribution of controlled substances.
- e) Records reflecting or relating to the transporting, ordering, purchasing, and/or

distribution of controlled substances, including but not limited to books, receipts, notes, ledgers, pay and owe sheets, correspondence, records noting price, quantity, date and/or times when controlled substances were purchased, possessed, transferred, distributed, sold or concealed.

f) Records reflecting or relating to co-conspirators, including but not limited to personal notes, correspondence, cables, telegrams, personal address lists, listings of telephone numbers, and other items reflecting names, addresses, telephone numbers, communications, and illegal activities of associates and conspirators in controlled substance trafficking activities.

g) Indicia or other forms of evidence showing dominion and control, or ownership of mail parcels, locations, vehicles, storage areas, safes, lock boxes, and/or containers related to the storage of controlled substances or proceeds.

VII. SEARCH OF DIGITAL INFORMATION

144. I am aware that users and vendors of online black markets use a computer to access the dark web where online black markets are located. I am also aware that individuals must use an electronic device to locate and communicate with bitcoin exchangers and purchase bitcoins. Users have to establish an account on an online black market's website to purchase goods and also establish accounts to initiate initial trades with bitcoin exchangers. Users also must establish electronic wallets to receive and send bitcoins to purchase drugs. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external or removable media, and/or computers. I am aware that once contact is made with a bitcoin exchanger on a digital currency exchange platform such as localbitcoins.com, all subsequent contact and transactions can be conducted from one phone to the other during a face to face transaction, exchanging currency for bitcoins. I am also aware that users can back-up wallets to paper printouts that would contain information to restore the wallet in an electronic form (cold storage). Passwords for access to online black markets, as well as for electronic wallets, are typically complex and are often written down or saved in an accessible manner on paper or on

some electronic device. I believe that these are located in the TARGET PROPERTY, TURRENTINE VEHICLE #1, TURRENTINE VEHICLE #2 and on the person of TURRENTINE.

145. As described above and in Attachment B, I submit that computers, smart phones, and possibly other storage media will be found within the TARGET PROPERTY, TURRENTINE VEHICLE #, TURRENTINE VEHICLE #2, and on the person of TURRENTINE and there is probable cause to search and seize those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. Furthermore, I submit that sufficient probable cause has been established to search and seize any online black-market vendor accounts, online digital currency exchange platform accounts, and the data contained therein. Due to the inherent illicit and anonymous nature of these accounts, and that there is no identified service provider for these accounts, legitimate, compliant or not, to which legal process may be served; I believe this to be the only manner to recover said evidence.

146. For example, based on my knowledge, training, and experience, I am aware that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches, physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

147. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a

storage medium can be stored for years at little to no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

148. Also, again based on my training and experience, wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

149. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their

use, who used them, and when.

150. Thus, the forensic analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

151. In cases of this sort, laptop computers and/or smartphones are also used as instrumentalities of the crime to commit offenses involving interstate drug sales and movement of drug proceeds. Devices such as modems and routers can contain information about dates, frequency, and computer(s) used to access the Internet. The laptop or smart phone may also have fingerprints on them indicating the user of the computer and its components.

152. Similarly, files related to the purchasing and selling of controlled substances, as well as, the movement of currency found on computers and other digital communications devices are usually obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the data, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary internet directory or "cache". The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

153. "User attribution" evidence can also be found on a computer and is analogous to

the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. I know from training and experience and discussions with other law enforcement officers that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of internet connection at the residence.

154. Searching the computer(s) for the evidence described in the attachment may require a range of data analysis techniques. For example, information regarding user attribution or internet use is located in various operating system log files that are not easily located or reviewed. In addition, a person engaged in criminal activity will attempt to conceal evidence of the activity by “hiding” files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this location (the computer) for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

155. Based upon knowledge, training and experience, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to

be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

156. The nature of evidence: As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a “booby-trap”), the controlled environment of a laboratory is essential to its complete and accurate analysis.

157. The volume of evidence and time required for an examination: Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

158. Technical requirements: Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on

the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

159. Variety of forms of electronic media: Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

160. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to, computer-assisted scans of the entire medium that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

VIII. REQUEST FOR SEALING

161. Finally, I respectfully request that this Court issue an order sealing, until further order of the Court, this case, to include, this Complaint, Arrest Warrant, Search Warrant Applications and Search Warrants, and all papers submitted to the Court in support of the foregoing. I believe that restricting these documents is necessary to protect the identity of cooperating individuals, because the items and information to be seized are relevant to an ongoing investigation into a criminal network, and not all of the targets of this investigation will be searched at this time. Restricting these documents is also necessary to prevent the potential destruction or concealment of evidence relevant to the underlying investigation, and premature disclosure could cause the target(s) of this investigation to attempt to destroy evidence, notify possible co-conspirators, or otherwise frustrate law enforcement efforts.

162. Based on my training and experience, I have learned that online criminals actively search for criminal Affidavits and Search Warrants via the Internet and disseminate them to

others actively seeking out information over the Web and other sources concerning law enforcement activity in this arena. Accordingly, premature disclosure of the contents of this Affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

IX. REQUEST FOR COMPLAINT AND ARREST WARRANT

163. Based on the foregoing, there is probable cause to believe that Jonathan Patrick TURRENTINE has violated the following federal statutes and I request respectfully that the Court issue a criminal complaint and warrant for his arrest:

- a) 21 U.S.C. § 841(a)(1) (Distribution of a Controlled Substance),
- b) 21 U.S.C. §§ 846, 841(a)(1) (Conspiracy to Distribute, and to Possess with Intent to Distribute, a Controlled Substance),
- c) 18 U.S.C. § 2320 (Trafficking in Counterfeit Goods and Services); and
- d) 18 U.S.C. § 1956(a)(1)(A)(i) (Money Laundering).

X. SEARCH WARRANT AUTHORIZATION REQUEST

164. Based on the facts set forth in this Affidavit, I believe there is probable cause to believe that evidence, fruits, proceeds, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (Distribution of a Controlled Substance), and 21 U.S.C. §§ 846, 841(a)(1) (Conspiracy to Distribute, and to Possess with Intent to Distribute, a Controlled Substance), 18 U.S.C. § 2320 (Trafficking in Counterfeit Goods and Services); and 18 U.S.C. § 1956(a)(1)(A)(i) (Money Laundering) are concealed in the locations identified in Attachments A-1 through A-4. Accordingly, I respectfully request, under Federal Rule of Criminal Procedure 41, that the Court issue search warrants authorizing the search of the locations described in Attachments A-1 through A-4, and the seizure of items described in Attachment B.

165. I also request that any vehicles under the control of the TURRENTINE are to be searched at the time these warrants are served, as evidenced by Department of Motor Vehicle registration information, possession of vehicles' keys, observations of the use of those vehicle by the occupants, and witness statements or admissions. Based on my training and experience, and

interaction with other law enforcement officers, I know that drug traffickers commonly transport and store the evidentiary items listed in Attachment B in their vehicles. I also know that these vehicles are not often registered to the person who has control over them.

I swear, under the penalty of perjury, that the foregoing information is true and correct to the best of my knowledge, information, and belief.

Respectfully submitted,

/s/ Christopher Scott Fitzpatrick

Christopher Scott Fitzpatrick,
Special Agent,
IRS-CI

Subscribed and sworn to me via telephone on: September 17, 2021

Allison Claire

The Honorable Allison Claire
UNITED STATES MAGISTRATE JUDGE

James R. Conolly

Approved as to form by
AUSA James R. Conolly

ATTACHMENT A-1
LOCATION TO BE SEARCHED

9161 Tuolumne Drive, Sacramento, California (TARGET PROPERTY)

A duplex residential property with a brown exterior, reddish-brown trim, and white garage door. The address numbers “9161” black in color and are affixed to the front exterior of the house between the front door and garage door. The property faces south and is located on the north side of Tuolumne Drive. The property to be searched is depicted in the recent photograph below.



The place to be searched includes all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, located on the **TARGET PROPERTY**; any computer, digital devices, and digital media located therein, where the items specified in Attachment B may be found; and all internal and external compartments and all containers that may be associated with the storage of controlled substances or the proceeds of the sales of controlled substances or their instrumentalities contained within the aforementioned places.

ATTACHMENT A-2
LOCATION TO BE SEARCHED

TURRENTINE VEHICLE #1 – Toyota Avalon bearing California license plate number 8WQS507 and Vehicle Identification Number (“VIN”) 4T1BF12B7VU171416, registered to Jonathan P. Turrentine.

The search of the **TURRENTINE VEHICLE #1** is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities contained within the aforementioned vehicle.

ATTACHMENT A-3
LOCATION TO BE SEARCHED

TURRENTINE VEHICLE #2 – Hyundai SUV bearing California license plate number 8UXX035 and Vehicle Identification Number (“VIN”) KM8JU3AC1CU441924, registered to S.T.

The search of the **TURRENTINE VEHICLE #2** is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities contained within the aforementioned vehicle.

ATTACHMENT A-4
LOCATION TO BE SEARCHED

Jonathan Patrick TURRENTINE – Further described as an adult Caucasian male, approximately 6’0” in height and 280 pounds, and including any wireless telephone he possesses, owns, maintains or operates (“Subject Phone”).



The search of the aforementioned person shall include any and all clothing and personal belongings, including backpacks, wallets, briefcases, and bags that are within Jonathan TURRENTINE’s immediate vicinity and control at the location where the search warrant is executed. It shall not include a body cavity or strip search.

This warrant authorizes the forensic examination of the Subject Phone for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as computers, hard drives, flash drives, tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute or contain evidence, instrumentalities, or fruits of violations of 21 U.S.C. § 841(a)(1) (Manufacture or Distribution of a Controlled Substance); 21 U.S.C. § 846 (Conspiracy to Manufacture, to Distribute, and to Possess with Intent to Distribute a Controlled Substance); Title 18 U.S.C. § 2320 (Trafficking in Counterfeit Goods and Services); Title 18 U.S.C. § 1956 (a)(1)(A)(i) (Money Laundering) from April 1, 2018 to present.

1. All records relating to the violations described above, including:
 - a. any and all documents, records or information relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of controlled substances;
 - b. any and all documents, records or information relating to the purchase, sale, importation, possession, shipment, tracking, delivery or distribution of packaging materials;
 - c. any and all documents, records or information relating to the purchase, sale, tracking, delivery or distribution of postage or express mail consignment;
 - d. any and all documents, records or information relating to the transfer, purchase, sale or disposition of virtual currency;
 - e. any and all documents, records, or information relating to the access, creation and maintenance of websites and hidden (Tor-based) services;
 - f. any and all documents, records, or information relating to email accounts used in furtherance of these offenses;
 - g. any and all records or other items which are evidence of ownership or use of computer equipment, including, but not limited to, sales receipts, bills for internet access, handwritten notes and handwritten notes in computer manuals.
 - h. any and all records relating to indicia of occupancy, residency, and ownership or use of the TARGET PROPERTY, TURRENTINE VEHICLE #1 and TURRENTINE VEHICLE #2, including,

but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase or lease agreements, identification documents, and keys;

i. any and all records of any address and/or telephone books, rolodex indicia, electronic organizers, telephone paging devices and the memory thereof, and any papers, records or electronic data reflecting names, addresses, telephone numbers, pager numbers of co-conspirators, sources of controlled substances and/or virtual currency, identifying information for customers purchasing controlled substances and/or virtual currency;

j. all bank records, checks, credit card bills, account information, safe deposit box information and other financial records;

k. all copies of income tax returns filed with the Internal Revenue Service (IRS) or the California Franchise Tax Board;

l. all records related to the purchase of real estate or other assets, or the leasing of storage units, and

m. financial records for including foreign and domestic banking records, ledger books, wire transfer instructions, and receipts for wire transfers.

2. Any digital devices or other electronic storage media and/or their components used as a means to commit the violations described above, including:

a. any digital device or other electronic storage media capable of being used to commit, further, or store evidence or fruits of the offenses listed above;

b. any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. any passwords, password files, seed words, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

3. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, seed words, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media; and

i. contextual information necessary to understand the evidence described in this attachment.

4. Records and things evidencing the use of an Internet Protocol (IP) address to communicate with the internet, including:

a. routers, modems, and network equipment used to connect computers to the internet;

b. records of Internet Protocol addresses used;

c. records of internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.

5. Any and all hidden services accounts or encrypted chat applications used in furtherance of the offenses described above, including, but not limited to, darknet market accounts, associated darknet forum accounts, Tor-based email accounts, and Wickr handles and logins.

6. Any and all peer to peer (P2P) virtual currency trading platform accounts, with no legitimate or identified service provider to which legal process may be served, used in furtherance of the offenses described above, including, but not limited to, localbitcoins.com accounts or bitcoin-otc internet relay chat channel accounts.

7. Virtual currency in any format, including but not limited to, wallets (digital and paper), seed words, usernames and passwords, public keys (addresses) and private keys.

8. Fiat currency (U.S. dollars or other government issued currency).

9. Keys to storage units, suites, lockers and safe deposit boxes.

10. Firearms or other prohibited weapons that are not registered to TURRENTINE or any of their cohabitants.

11. Controlled substances, associated paraphernalia and/or contraband, and any equipment or devices used in the manufacturing, storage and processing of controlled substances.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIME.

UNITED STATES DISTRICT COURT

for the
Eastern District of California

In the Matter of the Search of)

Hyundai SUV, with CA license plate 8UXX035
and VIN KM8JU3AC1CU441924)

Case No. 2:21-sw-0733 AC

SEALED

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ Eastern _____ District of _____ California
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-3, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before _____ October 1, 2021 _____ (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

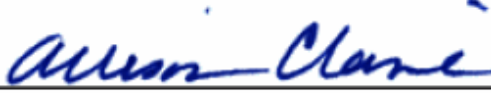
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: _____ September 17, 2021 at 10:17 a.m.

City and state: _____ Sacramento, California


ALLISON CLAIRE
UNITED STATES MAGISTRATE JUDGE

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date.

Signature of Judge

Date

ATTACHMENT A-3
LOCATION TO BE SEARCHED

TURRENTINE VEHICLE #2 – Hyundai SUV bearing California license plate number 8UXX035 and Vehicle Identification Number (“VIN”) KM8JU3AC1CU441924, registered to S.T.

The search of the **TURRENTINE VEHICLE #2** is to include all internal and external compartments and all containers that may be associated with the storage of controlled substances, proceeds of controlled substances sales, digital media, or their instrumentalities contained within the aforementioned vehicle.